**MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**P.O. Box 972-60200 – Meru-Kenya.**

 **Tel: 020-2069349, 061-2309217. 064-30320 Cell phone: +254 712524293, +254 789151411**

**Fax: 064-30321**

**Website:** [**www.must.ac.ke**](http://www.must.ac.ke) **Email:** **info@must.ac.ke**

**University Examinations 2015/2016**

FOURTH YEAR, FIRST SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY, BACHELOR OF BUSINESS INFORMATION TECHNOLOGY

AND

THIRD YEAR, FIRST SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER TECHNOLOGY

**CCS 3475: COMPUTER SECURITY AND CRYPTOGRAPHY**

**DATE: NOVEMBER 2015 TIME: 2 HOURS**

**INSTRUCTIONS:** *Answer question* ***one*** *and any other* ***two*** *questions*

**QUESTION ONE (30 MARKS)**

1. Using this Playfair matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| M | O | N | A | R |
| C | H | Y | B | D |
| E | F | G | I/J | K |
| L | P | Q | S | T |
| U | V | W | X | Z |

Show how you can encrypt the message “we are discovered, save yourself” (10 Marks)

1. What is the difference between a block cipher and a stream cipher? (5 Marks)
2. Explain the following types of malicious software (6 Marks)
3. Worms
4. Trojans
5. Logic bombs
6. An important aspect of security is user education; describe the main points that you would cover if you were asked to give a presentation on password management to all the employees in your company. (3 Marks)
7. Discuss the following computer security services (6 Marks)
8. Confidentiality
9. Integrity
10. Availability

 **QUESTION TWO (20 MARKS)**

1. Describe the following two types of IDS (4 Marks)
2. Network-based IDS
3. Host-based IDS
4. Given the access control matrix shown below generate and discuss the following

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Object Subjects/groups | R1 | R2 | R3 | R4 |
| A | W | R | R | W |
| B | R |  |  |  |
| Group G1 | W |  |  |  |
| Group G2 |  | W |  |  |
| C |  |  |  | R |

1. Access control list (5 Marks)
2. Capability list (5 Marks)
3. Differentiate between Rule based access control and Role based access control (4 Marks)
4. Discuss why computer security remains a challenge despite the efforts being put by the organizations (2Marks)

**QUESTION THREE (20 MARKS)**

1. Alice and Bob have agreed to use the Diffie Hellma key exchange mechanism. Explain how this system works. Given the p=37 and g=13, show how this mechanism can be used to send keys secretly. (10 Marks)
2. Using a diagram discuss the Model of Conventional Encryption (10 Marks)

**QUESTION FOUR (20 MARKS)**

1. Using Caesar cipher encrypt the message “meet me after the toga party” (6 Marks)
2. What are **two** problems with the one-time pad? (4 Marks)
3. Discuss any **five** components of good security policy (10 Marks)

**QUESTION FIVE (20 MARKS)**

1. Decipher the message *DR GREER ROCKS* using the Hill cipher with the inverse key
2. 3
3. 1

Show your calculations and the results. (14 Marks)

1. Discuss the following terms as used in computer security (6 Marks)
2. Computer security
3. Threat
4. Vulnerability